CLAIMS

Sub B10

1. A method of distributing digitially encoded data, comprising

a) dividing said data into a multiplicity of frames,

b) encrypting said frames,

c) distributing multiple copies of the said data frames to a multiplicity of users,

d) communicating a seed value for key generation to respective secure modules located at each of the multiplicity of users,

e) decoding the data frames at respective users using keys derived from the seed value communicated to the secure module,

f) passing a control message to the secure module at a selected one or more of the multiplicity of users,

g) at the or each selected user, in response to the said control message, controlling the availability of keys generated from the said seed value, thereby controlling access by the users to the said data.

2. A method according to claim 1, in which a control field is distributed to each of the multiplicity of users, and the secure module is arranged to enable decryption of a respective frame only when the said control field has been passed to the secure module.

3. A method according to claim 2, in which the said control message for modifying the availability of keys is communicated to the secure module in the said control field.

a

4. A method according to claim 1 ~~any one of the preceding claims~~, in which each data frame includes a frame identity field, and each key generated by the secure module is specific to one frame identified by the said field.

a

5. A method according to claim 1 ~~any one of the preceding claims~~, in which the step of distributing multiple copies of the said data comprises multicasting packets of data via a communications network to the plurality of users.

a

6. A method according to ~~any one of the preceding claims~~ claim 1, in which the control message is distributed with a data frame to the multiplicity of users, a user identity field identifying a selected user or group of users is included in the control message, and the control message is acted on only by the user or group of users identified by the said user identity field.

a

7. A method according to ~~any one of the preceding claims~~ claim 1, in which the control message includes a stop flag, and in response to the stop flag the generation of keys at the or each selected user is stopped.

a

8. A method according to ~~any one of the preceding claims~~ claim 1, including returning a response signal from the secure module to the source of the control message.

9. A method according to claim 8, in which the control message includes a contact sender flag, and the step of returning a response signal from the secure module is carried out when the contact sender flag is set.

a

10. A method according to claim 8 ~~or 9,~~ including transmitting a further control message to the user on receipt of the said response signal.

11. A method of operating a customer terminal in a data communications system, the method comprising:

a) receiving at the customer terminal a multiplicity of encrypted data frames

b) receiving at the customer terminal a seed value for key generation

c) passing the said seed value for key generation to a secure module located at the customer terminal

d) generating in the secure module using the seed value keys for the decryption of data frames;

e) decrypting the data frames using the said keys;

f) passing to the said secure module a control message received from a source remote from the customer terminal;

g) in response to the said control message controlling the availability of keys generated using the said seed value and thereby controlling access by the user of the customer terminal to data received at the customer terminal.

B10

12. A data communications system comprising

a) a remote data source arranged to output a plurality of frames;

b) encryption means for encrypting the plurality of frames with different respective keys;

c) a communications channel arranged to distribute multiple copies of the encrypted data frames ;

d) a multiplicity of customer terminals arranged to receive from the communications channel respective copies of the encrypted data frames;

e) a key generator located at a customer terminal and programmed to generate from a seed value keys for use in decrypting data frames:

f) key control means connected to the key generator, the key control means comprising:

an interface for receiving control messages; and

control means responsive to the said control messages and arranged to control the availabiltiy to the user of keys generated from the seed value; and

g) decryption means connected to the key generator and arranged to decrypt the data frames received at the customer terminal from the communications channel.

13. A data communications system according to claim 12, in which the communications channel is a packet-switched data network.

a

14. A customer terminal for use in a method according to ~~any one of claims 1 to 11~~ claim !, the customer terminal comprising:

a) a data interface for connection to a data communications channel;

b) a key generator programmed to generate from a seed value keys for use in decrypting data frames:

c) key control means connected to the key generator, the key control means comprising:

RID

an interface for receiving control messages; and

control means responsive to the said control messages and arranged to control the availabiltiy to the user of keys generated from the seed value; and

d) decryption means connected to the data interface and to the key generator and arranged to decrypt data frames received via the data interface.

a

15. A data server for use in method according to claim 1 ~~any one of claims 1 to 10~~, the data server comprising:

a) a data interface for connection to a data communications channel:

b) means for outputting encrypted data frames via the data interface onto the communications channel for receipt by a multiplicity of customer terminals;

c) means for outputting control mesages onto a data communications channel for controlling the operation of key generators at customer terminals.

a

16. A method according to claim 1 ~~any one of claims 1 to 11~~, including generating keys from the seed value by iterated operations on the seed value by selected ones of a plurality of predetermined functions.

17. A method of decrypting data frames characterised by generating a decryption key from a seed value by iterated operations on a seed value by selected ones of a plurality of predetermined functions.

a

18. A method according to claim 16 ~~or 17~~, in which the selection of the said predetermined functions is determined by the value of a frame identity number.

a

19. A method according to claim 16 ~~any one of claims 16 to 18,~~ in which the predetermined functions are computationally symmetric.

20. A method according to claim 19 in which the said functions are left-shifted binary XOR and right-shifted binary XOR.

a

21. A method according to ~~any one of claims 1 to 11 and 16 to 20,~~ claim 1 including applying different characteristic variations to data decrypted at different respective customer terminals.

a B10

22. A method or system according to ~~any one of the preceding claims,~~ claim 1 including a plurality of remote data sources, each outputting a respective plurality of frames.

23. A method or system according to claim 22, in which the customer terminal receives a primary seed value common to different respective data streams from the plurality of data sources, and derives from the common primary key a plurality of different respective secondary seed values for decrypting frames from different respective data sources.

24. A method or system according to claim 23, in which data received from different data sources includes different respective source identity values, and the respective secondary seed value is generated from the primary seed value by modifying the primary seed value with the source identity value.

a

25. A method according to ~~any one of claims 1 to 11 and 18 to 21,~~ claim 1 in which each data frame includes a frame type field.

26. A method according to claim 25, including storing a receipt including data from the frame type field.

27. A method of distributing digitially encoded data, comprising

a) dividing said data into a multiplicity of frames,

b) encrypting said frames,

c) marking frames with a frame type field

d) communicating said data frames to a user

d) communicating a seed value for key generation to the user

e) decoding the data frames at the users using keys derived from the seed value

f) generating and storing receipts for said data frames, said frames including frame type data from the frame type field.

B30

~~28. A method according to claim 27, further comprising communicating receipts to a third party, and obtaining from the said third party a payment for receipt of data of a specified type.~~